Coloquio Inst-Mat
Instituto de Matemáticas
Universidad de Talca
Camino Lircay S/N, Campus Norte, Talca-Chile

Cálculo de orden de grupo en curvas de género 2

Nicolas Thériault*
Departamento de Matemáticas
Universidad de Santiago de Chile

Abstract

Las curvas hiperelípticas de género 2 son de interés para varias aplicaciones criptográficas. Un problema importante para la utilización de esas curvas consiste en encontrar una curva cuyo orden de grupo sea "bueno" (idealmente de orden primo con un twist cuadrático de orden primo también). Varios resultados obtenidos los últimos años nos permiten mejorar los tiempos de cálculos del orden de grupo de una curvas hiperelípticas de género 2 por un orden de magnitud, dejando esas curvas mucho más accesibles. En esta charla, presentaremos algunas de las herramientas desarrolladas para lograr estas mejoras.

*e-mail: nicolas.theriault@usach.cl